Journal of Information Security, **2013, 4, 213-224**
http://dx.doi.org/10.4236/jis.2013.44024 Published Online October 2013 (http://www.scirp.org/journal/jis)

Analysis of Malware Families on Android Mobiles: Detection Characteristics Recognizable by Ordinary Phone Users and How to Fix It

Hieu Le Thanh[1,2]
[1]School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, China
[2]Hue University's College of Education, Hue, Vietnam
Email: Hieudhsphue2002@yahoo.com

Received April 9, 2013; revised May 11, 2013; accepted May 19, 2013

ABSTRACT

The sale of products using the android Operation System (OS) phone is increasing in rate: the fact is that its price is cheaper but its configured hardware is higher, users easily buy it and the approach to this product increases the risk of the spread of mobile malware. The understanding of majority of the users of this mobile malware is still limited. While they are growing at a faster speed in the number and level of sophistication, especially their variations have created confusion for users; therefore worrying about the safety of its users is required. In this paper, the author discussed the identification and analysis of malware families on Android Mobiles. The author selected the recognizable characteristics from ordinary users with their families collected from 58 malware families and 1485 malware samples and proposed solutions as recommendations to users before installing it with the ultimate desire to mitigate the damage in the community that is on the android phone, especially the ordinary users with limited understanding about potential hazards. It would be helpful for the ordinary users to identify the mobile malware in order to mitigate the information security risk.

Keywords: Mobile Security; Android Malware Families

1. Introduction

In recent years, Sales of products using Android phones have continued to accelerate. Specifically in 2012, phones which use the android operating system rose from 52.5% to 72.4% compared to 2011, while the IOS operating system fells from 15% to 13.9% compared to 2011, according to Gartner [1]. Some applications of the android operating system from Android Market are growing to compete with the largest application. Now Apps store is developed by third—party market, not to mention the thousands of everyday applications. According to Xyologic: "Android to overtake Apple soon", Apple's App store has now reached 25 billion downloads, Android's App store has now reached 10 billion downloads, but both tracked at 1 billion downloads a month [2].

This increases the amount of malicious software on the Android operating system. According to security Kaspersky Labs, in the second quarter of 2012 the mobile malware increased in three folds. In 2012, 99% of all the mobile malware they detected every month was designed for Android. The most widespread malicious objects detected on Android smartphones can be divided into three main groups: SMS Trojans, advertising modules and exploits to gain root access to smartphones [3]. Specifically, 40% of modern smartphone owners do not use antivirus software [4].

Whilst malware is growing rapidly, a number of ordinary users that have easy access to the smartphone device do not have basic understanding of the potential danger. So we need to have the classification of samples according to similar characteristics, as well as collect more new malware to create malware families. Then, we can analyze it fully to make recognizable signs from ordinary users and guard solutions to mitigate the threats of the impact and risk of malwares before installing it from official android market or third-party market.

In this paper, the author first discussed the feature to select a sample of malware families and method to analysis them. Next, in Section 2, the author presented methods and tools to analyse malware samples. In section 3, the author presented some selected results of the features that ordinary users can easily recognize. From the analysis on the samples, the author collected the list from the project, blog and threat reports of antivirus companies [5,6] (including existing malware families and add them every day) and the threats that malicious applications can do. Section 4 shows the detection results with ten representatives of mobile phone antivirus software. In Section 5, the author discussed six (6) steps to security android phones. Finally, Section six (6) is the summary.

2. Methods and Tools to Analyze Malware Samples

In this section, the author first discussed the feature to select a sample of malware families and methods to analyses them.

2.1. Malware Family

Malware family feature that comes to notice is that of closeness which certain traits are preserved, including: similar activation, facial features, hereditary diseases and a host of other commonalities.

One of the variations which is most harmful is KungFu malware family. There are variations with different names KungFuA (KungFu1), KungFuB (KungFu2), KungFuC (KungFu3), KungFuD (KungFu4), KungFuE (KungFu Sapp) or KungFu Lena (Legacy Native) with properties which are analysed as follows:

All KungFu malwares are packaged and downloaded from third markets and fora. It adds into applications a new service and a new receiver. With privilege root exploits, it automatically launches the service so that it doesn't interact with the user. KungFu can collect information on the infected mobile phone, including IMEI number, phone model, version of Android OS. The first variant, KungFuA exploits Dalvik codes based on Java and a single C&C server and payload is encrypted with AES. Differently, KungFuB exploits native code and three C&C servers. KungFuC inherits from KungFuB, it exploits vulnerability to allow local users to gain privilege by sending a NETLINK message (CVE-2009-1185) [7]. KungFuD inherits from KungFuA and encrypted its native binaries. KungFuE inherits from KungFuD and encrypting a few strings to obfuscate its code and use a custom certificate in official market [8-10]. "DroidKung-Fu" variants structure mentioned in **Figure 1**.

Its purpose is to evade the detection of mobile antivirus software. So the virus software is difficult to effectively detect variants with a rate of 100%.

2.2. Methods and Tools to Analyze Android Mobile Malware Sample

Common method for analysing malware in android OS is reverse engineering. Reverse engineering is the process of discovering the technological principles of a device, object, or system through analysis of its structure, function, and operation [10]. Android OS was developed by Google and is based upon the Linux kernel and GNU software in which the malware application package files use the apk extension. They include all of the application's code (.dex files), resources, assets, and manifest file. Dex file (Dalvik Executable) is compiled Android a-pplication code file. Tools that focus three groups on examining inner-workings of Android mobile applications:

1) Command line:

- Tool to unpack the .apk file: Winzip, Rar
- Tool to get the bytecode from the .dex file: *for example*, smali to compile and baksmali to decompile (or dex2jar and jd-gui), dexdump…

The author analysed a sample (RU .apk) below:

Step 1: The malware is an apk package extract of its content, show example **Figure 2**.

Step 2: Use smali .rar to compile smali file: extracted the byte code from classes .dex file, show example **Figure 3**.

Step 3: Open code contained in the MoviePlayer.smali file. You can discover the purpose of it, show example **Figure 4**.

2) Software to compile and decompile:

- Compile: Java code, smalicode and .dex: for example APKtoJava.

We analysed a sample (RU .apk) below:

Step 1: open APKtoJava (show **Figure 5**).

Step 2: open class java to read program file (show example **Figure 6**).

3) Using website: for example http://anubis.iseclab.org

He analysed a sample (*RU .apk*) *below*:

Choose file apk website to analyse, show example **Figure 7**.

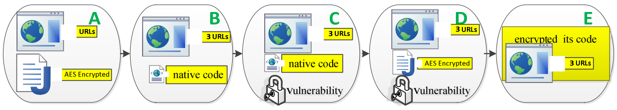
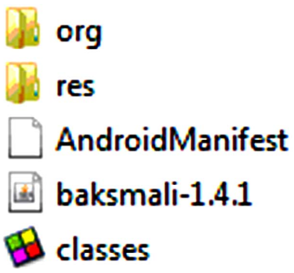
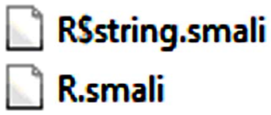


Figure 1. "DroidKungFu" variants structure.



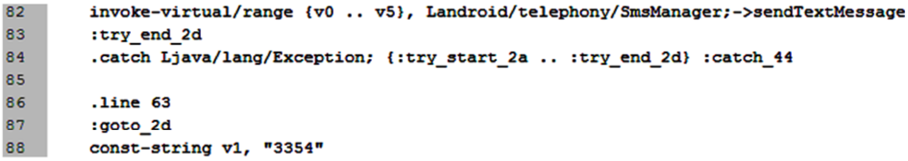
org
res
AndroidManifest
baksmali-1.4.1
classes

Figure 2. Classes is dex file to analyze.



R$string.smali
R.smali

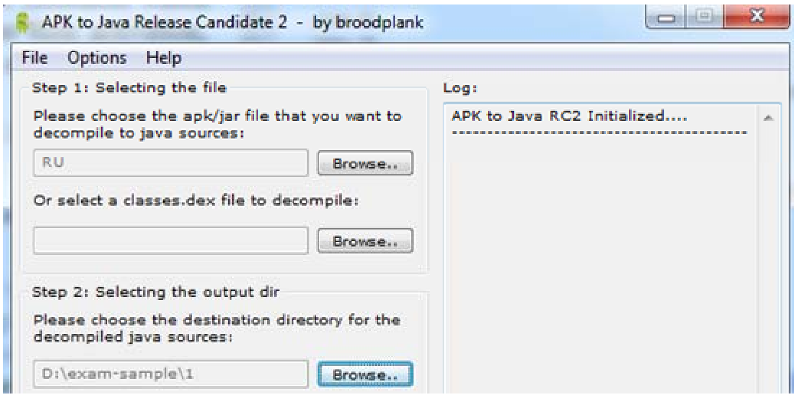
Figure 3. Movie player. Smali is main code of malware.



```
invoke-virtual/range {v0 .. v5}, Landroid/telephony/SmsManager;->sendTextMessage
:try_end_2d
.catch Ljava/lang/Exception; {:try_start_2a .. :try_end_2d} :catch_44

.line 63
:goto_2d
const-string v1, "3354"
```

Figure 4. Malware send a message to phone number 3354.



Step 1: Selecting the file

Please choose the apk/jar file that you want to decompile to java sources:

RU

Browse..

Or select a classes.dex file to decompile:

Browse..

Step 2: Selecting the output dir

Please choose the destination directory for the decompiled java sources:

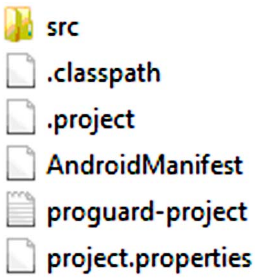
D:\exam-sample\1

Browse..

Log:

```
APK to Java RC2 Initialized....
----------------------------------------
```

Figure 5. Screen of APK tool to decompile to java sources.



src

.classpath

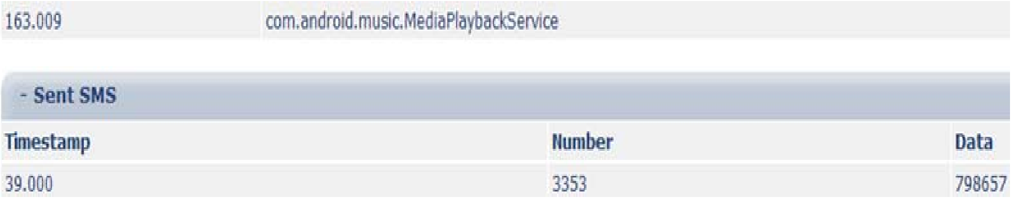
.project

AndroidManifest

proguard-project

project.properties

Figure 6. A Class java sources after decompile by APK tool.



163.009	com.android.music.MediaPlaybackService

- Sent SMS

Timestamp	Number	Data
39.000	3353	798657

Figure 7. An analysis result for file RU .apk from website.

3. Results of the Features That Ordinary Users Easily Recognize

In the process of analysing the samples the author collected, the author had encountered difficulties with different names of the first authors found it. So his statistics record all the different names for easy sorting into their malware families. In addition to describing the visible symptoms, the author used illustrations or icons in **Table 1**.

Besides, Symptoms of malware which exploits the device to gain root privilege are not easily visible. So we propose to use mobile Security software solutions in the next chapter, with some assessment test results with our samples set.

Statistical results below with reference from the first detection of the authors in manufacturer's anti—virus software: Symantec, NQMobile, F-secure, Lookout, Kaspersky, AVG, … and projects related links, Blog: http://www.csc.ncsu.edu/faculty/jiang, http://www.fortiguard.com,http://androguard.blogspot.com, http://blog.fortinet.com/... [10-52].

In the first column of **Table 4**, the author collected the different names of the same malware families [5,52] by different anti-virus companies, based on installation methods, activation mechanisms or the name of the mali-

Table 1. Describes characterization and area of the effects of malware families.

Area (**)	Malware Familes	Description (*)											
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
CN	AnserverBot	x						x					
CN	BaseBridge (AdSMS)	x		x				x					
	BeanBot	x						x					
	Pjapps	x	x	x				x					
	BGSERV	x	x	x				x					
	CruseWin (CruseWind)							x		x			
CN	DroidCoupon	x						x					
	DroidDeluxe			x							x		
	DroidDream (DORDRAE)			x				x					
	DreamLight	x						x					
	DroidKungFu (LeNa)	x			x	x		x					
	Smssend (fakeplayer)							x		x			
CN	gamblersms	x						x					
	Geinimi	x		x				x					
USA, CN, RU	GGTracker	x		x				x		x			
CN	GingerMaster (GingerBreaker)								x		x		
	GoldDream	x		x				x					
	Gone 60 (gonein 60)	x		x				x					
	GPSSMSSpy (mobinauten, SmsHowU, smsspy)						x						
CN	HippoSMS							x		x			
	Jifake					x				x			x
	jSMSHider (smshider, Xsider)							x	x				
CN	KMin (ozotshielder)	x	x					x					
	LoveTrap (cosha, Luvrtrap)	x					x	x		x			
	Nickyspy (Nickispy)			x			x	x					
	Plankton				x	x	x	x					
	RogueLemon					x		x					
	RogueSPPush					x		x					
	SMSReplicator			x				x					
	SndApps	x		x				x					
	Spitmo	x						x				x	
	Tapsnake						x	x					
	Walkinwat	x		x			x	x					
	YZHC							x		x			
	zsone							x		x			

Continued

	Battery Doctor (fakedoc)					x		x					
	CI4					x		x					
	Counterclank		x					x					
JN	Dougalek	x		x				x					
E. EU	DropDialer			x				x		x			
CN, CAN	FakeAngry (AnZhu)	x			x			x					
	Faketimer (oneclickfraud)	x						x					
Spain	FakeToken	x						x		x			
RU	FindAndCall			x				x					
	Gamex (muldrop)					x							
RU, EU	Logastrod	x				x		x		x			
	Luckycat	x	x					x					
	Moghava				x								
ME. EU	Notcompatible	x						x					
RU	Opfake							x		x			
CN	Rootsmart (Bmaster)	x						x			x		
	Steek (fakelottery, atakr)	x				x		x					
	VDloader	x	x					x		x			

(*): Details **Table 1** are described in **Table 2**. (**): Details **Table 1** are described in **Table 3**.

Table 2. Gives detailed explanation of stolen information activities of malware.

Num	Description
1	Steal personal information: IMEI, IMSI and phone number
2	Steal Net information: history and bookmarks, APN, IP, Mac
3	Steal phone’s state: calls log, SMS, contacts, account
4	Steal file information: change or copy file in external storage
5	Steal apps information: download and install apps
6	Stolen location information: GPS, Google, Country code
7	Send information to A C&C server (SMS messenger)
8	Send information to URL (by connecting internet.)
9	Send to premium-rate SMS messages
10	Exploits root
11	Steal banking codes: mTAN
12	Steal QR code

Table 3. Abbreviated name of areas.

Area: High risk Of infection	Description
CN	China
USA	America
Ru	Russia
JN	Japan
EU	Europe
CAN	Canada
E	Eastern
ME	Middle East

cious packaged applications added. This solved problem of naming schemes of malware families such as [5]: “Last but not least, during the process of collecting malware samples into our current dataset, we felt confusions from disorganized or confusing naming schemes”.

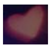
From visible symptoms malware families in **Table 5**, the author proposes some specific criterion for identifying the mobile malware:

Ordinary phone users can recognize several features such as: premium-rate services and phone bill abnormal increase, display of a black screen, automatically install a software in which its users has not requested, or without a launcher icon after installation in applications list, warning requirements application not licensed and crack

Table 4. Description about visible symptoms of malware.

Families	Visible Symptoms	Manually Checked by user	Illustrations
AnserverBot	It makes a new dialog to request and upgrade a new apps but does not show any icon.	You remember new apps name and check show icon on your home screen (request upgrade)	
BaseBridge (AdSMS)	Abnormally, high bill to connect internet from data connect or GPRS. 360 Safeguard is installed additional.	Check the regular phone bill. Error message from 360 Safeguard or show 360 Safeguard icon	
BeanBot	The device booting up or hanging up on a phone call.	Check the regular phone bill.	
Pjapps	Request read/write Browse's history and bookmarks and receive SMS when you install it.	View Request read/write Browse's history and bookmarks and receive	
BGSERV	Android market security is running by BgService.	View BgService is running when you don't request	
CruseWin (CruseWind)	Display of a black screen.	Check the regular phone bill. Can view: Flash MMS icon or Flash icon	
DroidCoupon	It uses a popular root exploit—" Rage against the Cage" in Android 2.2 and earlier, hide Platform so we are difficult to detect it.	Phone upgrade to a higher version	
DroidDeluxe	Install password recovery tool. It will not work on android 2.3, with message: "This application has stopped unexpectedly. Please try again".	You can detect it when your phone using version 2.3. View Recovery Deluxe tool	
DroidDream (DORDRAE)	It also disguises itself as apps like battery-monitoring tool, a task-listing tool, and an app listing the permissions used by installed apps.	View my Batter Life	
DreamLight	Service named "CoreService" running. Getting a phone call.	View Illustrations	
DroidKungFu (LeNa)	Install Google search or Google Ssearch.	View Icon 2 apps: Google search or Google Ssearch	
Smssend (fakeplayer)	Running media player application.	Check the regular phone bill. Auto run media player	
gamblersms	Request provide a phone number and an email address.	View: Phone number and email	
Geinimi	Create a shortcut, Change wall paper Appear a popups message about Google map.	check for abnormal appearance on the background	
GGTracker	Website analyzing the phone's battery or request download APK solution battery.	View solution battery	Battery Information Battery:65% Current Saving Mode: Normal Mode
GingerMaster (GingerBreaker)	Requires add apps list.	Your phone using Android 2.3/2.3 Requires add apps list	
GoldDream	Difficult to identify. You should use anti-virus software. If detects it, you should uninstall apps.		
Gone60 (gonein60)	Pay money from web gi60s.com	Self-uninstallation as figure beside: Enter this code (5-digit code) to gi60s.com (send a website)	
GPSSMSSpy (mobinauten, SmsHowU, smsspy)	The message the spy sends (How are you) is an error or spam.		
HippoSMS	Costs bill from the beginning of 1066.	Check the regular phone bill.	
Jifake	Open link to download file apk, rar, but don't see is that files.	Check the regular phone bill.	
jSMSHider (smshider, Xsider)	"InstallService" service named appeared in Application Manager but don't install.	View Illustrations: "InstallService"	
KMin (ozotshielder)	Changes the Live Wallpape.	View two icons	
LoveTrap (cosha, Luvrtrap)		Check the regular phone bill.	
Nickyspy (Nickispy)	Install Google + application	View Google + application	
Plankton	Removal of installed mobile security software.	Check security software in the system tray or the main screen	

Continued

RogueLemon	Request subscribed value-added service.	Check your phone bill	
RogueSPPush	Request subscribed value-added service.	disagree registration value-added services. Check Your phone bill Show RogueSPPush love app.	
SMSReplicator	Ask a question your interested issues through messages to other phone.	View Alert: Phone Number(s) to answer o another phone number	
SndApps	Built-in: the user clicks this icon with "FREE" and "No Ads" in their descriptions download and install.	View built-in	
Spitmo	See a pop up "Certificate update" or "security" apps.	View Settings: 1 process and popup number	
Tapsnake	If you click Menu button then appear prompted to registrate your information.	Stop SnakeService: Settings/Applications/Running Service, choose SnakeService to Stop.	
Walkinwat	Application Not Licensed Cracking...	You should not choose a crack for apps suggestions (Alert).	
YZHC	Abnormally high bill from SMS sending and connection Internet.	Check regularly phone bill and your account	
zsone	Abnormally high bill from SMS sending .	Check regularly phone bill and your account	
Battery Doctor (fakedoc)	pop-up ads about improve your battery life.	You should not install scare or trick app that you don't need. (Battery Doctor)	
CI4	Without a launcher icon after installation.		
Counterclank	Restrict the use of ad networks.		
Dougalek	An error has occurred and the video has not loaded.		
DropDialer	Uninstall itself after sending.	Check regularly phone bill and your account. Check icon apps after installed a app.	
FakeAngry (AnZhu)	Pop-ups displayed Bookmark Name/Bookmark URL.	Appear Screen Off And Lock apps	
Faketimer (oneclickfraud)	Opens unhealthy content websites.	Remove its	
FakeToken	uses the logo and colours of the bank in the icon of the application when the user don't enter the first factor of authentication then shows an error	Icon of Bank: Santander, BBVA, Banesto,..	
FindAndCall	the app sends SMS spam	View icon apps (Find & call). Remove it	
Gamex (muldrop)	Appear new icon apps and Message in Android 8.2.3 patch	View Android 8.2.3 patch	
Logastrod	Abnormally high bill	Check regularly phone bill	
Luckycat	an "empty" icon or a standard Android icon		
Moghava	JPG images increasing in size: full sdcard	uninstalling the app delete jpg	
Notcompatible	Request open "Unknown sources"	Download from Android market	
Opfake	Its variant have the Opera icon	strange charges to your phone bill	
Rootsmart (Bmaster)	"Settings" icon with Chinese name	"Settings" icon Chinese name	
SteeK (Fatakr, fakelottery)	money the user needs to pay if he wants to participate for applications or gaming	Check regularly phone bill	
VDloader	no corresponding icon in the phone's app	A 3D waterfall wallpaper	

them, …

However, malicious software is not a software bug so when installing or running the software, you should consider bug occurrence with above several features.

4. Detection Results of Malware Families

The author installed four mobile security software from Lenovo Store on a Lenovo phone P70 (version 2.3.5) to

Table 5. Detection results from top anti-virus software 2012.

Malware Families	Num	Dr. Web			Kaspersky			NQ/NetQin			Zoner		
		Num	**time**	**%**	**Num**	**time**	**%**	**Num**	**timer**	**%**	**Num**	**time**	**%**
AnserverBot	190	190	128	100	169	93	88.9	2	36	1.1	190	9	100
BaseBridgeA.B.C	126	121	86	96.0	124	134	98.4	61	6	48.4	126	11	100
BeanBot	8	0	1	0.0	0	12	0.0	0	1	0.0	8	3	100
Bgserv	10	10	2	100	10	12	100	1	2	10.0	10	1	100
CruseWin (CruseWind)	2	2	1	100	2	1	100	0	1	0.0	2	1	100
DroidCoupon	1	0	1	0.0	1	0	100	0	1	0.0	0	1	0.0
DroidDeluxe	3	1	1	33.3	2	1	66.7	3	2	100	2	1	66.7
DroidDream (DORDRAE)	26	26	7	100	26	5	100	22	4	84.6	26	2	100
DroidDreamLight	47	47	9	100	17	16	36.2	12	5	25.5	47	4	100
DroidKungFu1 (KungFuA, fokonge, gongfu)	34	34	18	100	34	14	100	33	7	97.1	34	5	100
DroidKungFu2 (KungFuB)	32	32	9	100	32	12	100	5	7	15.6	32	3	100
DroidKungFu3 (KungFuC)	310	309	178	99.7	205	338	66.1	0	74	0.0	310	40	100
DroidKungFu4 (KungFuD)	96	96	54	100	44	274	45.8	96	0	100	96	12	100
DroidKungFuSapp (KungFuE)	3	3	1	100	0	7	0.0	0	2	0.0	3	1	100
FakePlayer (SMSSend)	7	7	1	100	7	2	100	3	1	42.9	7	1	100
GamblerSMS	1	0	1	0.0	0	0	0.0	0	1	0.0	1	1	100
Geinimi	109	97	63	89.0	79	133	72.5	109	41	100	109	15	100
GGTracker	3	3	1	100	3	183	100	0	1	0.0	3	1	100
GingerMaster	4	4	1	100	4	2	100	0	1	0.0	4	1	100
GoldDream (spygold)	49	49	35	100	29	140	59.2	12	12	24.5	49	4	100
Gone60 (gonein60)	14	13	1	92.9	14	8	100	0	2	0.0	14	1	100
GPSSMSSpy (mobinautn, SmsHowU, smsspy)	6	6	2	100	4	1	66.7	0	1	0.0	6	1	100
HippoSMS	4	3	1	75.0	1	1	25.0	2	1	50.0	4	1	100
Jifake	1	1	1	100	1	0	100	0	1	0.0	1	1	100
jSMSHider (smshider)	16	16	5	100	16	16	100	11	3	68.8	16	2	100
KMin (ozotshielder)	100	52	39	52.0	93	124	93.0	0	35	0.0	100	9	100
LoveTrap (cosha)	1	1	1	100	1	2	100	1	1	100	1	1	100
NickySpyABC	3	3	1	100	3	2	100	0	1	0.0	3	1	100
Pjapps	81	60	42	74.1	67	98	82.7	80	21	98.8	81	13	100
Plankton (tonclank)	61	29	12	47.5	11	156	18.0	6	29	9.8	61	10	100
RogueLemon	2	0	1	0.0	0	5	0.0	0	2	0.0	2	1	100
RogueSPPush (autospsubscribe)	9	9	2	100	6	23	66.7	0	4	0.0	9	1	100
SMSReplicator	1	1	1	100	1	0	100	0	1	0.0	1	1	100
SndApps	10	10	3	100	8	6	80.0	1	1	10.0	10	1	100

Continued

Spitmo (zitmo)	1	1	1	100	1	2	100	0	1	0.0	1	1	100
Tapsnake	2	2	1	100	2	2	100	0	1	0.0	2	1	100
Walkinwat	1	1	1	100	1	4	100	0	1	0.0	1	1	100
YZHC (uxipp, wukong)	24	21	6	87.5	13	29	54.2	5	4	20.8	24	2	100
Zsone	12	12	3	100	12	9	100	11	3	91.7	12	1	100
.Battery Doctor (fakedoc)	1	1	1	100	1	2	100	0	1	0.0	1	1	100
CI4 SMS Bot	1	0	1	0.0	0	1	0.0	0	1	0.0	1	1	100
Counterclank	6	6	2	100	0	27	0.0	0	5	0.0	6	2	100
Dougalek (dougaleaker)	6	0	1	0.0	0	1	0.0	0	1	0.0	6	1	100
DropDialer	2	0	1	0.0	0	5	0.0	0	1	0.0	2	1	100
FakeAngry (AnZhu)	1	1	1	100	0	1	0.0	0	1	0.0	1	1	100
Faketimer (oneclickfraud)	4	3	1	75.0	0	1	0.0	0	1	0.0	3	1	75.0
FakeToken	1	1	1	100	0	1	0.0	0	1	0.0	1	1	100
FindAndCall	1	0	1	0.0	0	1	0.0	0	1	0.0	1	1	100
Gamex (muldrop)	1	1	1	100	0	1	0.0	0	1	0.0	1	1	100
Logastrod	4	4	1	100	0	1	0.0	0	1	0.0	4	1	100
LUCKYCAT	1	0	1	0.0	0	1	0.0	0	1	0.0	0	1	0.0
Moghava	1	1	1	100	0	12	0.0	0	3	0.0	0	1	0.0
notcompatible	1	1	1	100	0	1	0.0	0	1	0.0	1	1	100
opfake	7	2	1	28.6	0	6	0.0	0	2	0.0	4	1	57.1
ROOTSMART	13	2	0	15.4	1	27	7.7	3	5	23.1	13	1	100
SMSZombie	8	8	2	100	0	11	0.0	0	2	0.0	7	2	87.5
Steek (fakelottery)	14	0	1	0.0	0	49	0.0	0	8	0.0	14	3	100
VDloader	2	0	1	0.0	0	9	0.0	0	2	0.0	2	1	100
Total samples	1485	1303	742	87.7	1045	2025	70.4	479	357	32.3	1476	190	99.4

assess the effectiveness test on the same configuration and the same phone, the same samples set. (Dr. Web Anti-virus v7.00.3 (Dr. Web), Kaspersky Mobile Security. 9.10.139 (Kaspersky), NQmobile antivirus v5.2 (NQ or NetQin) and Zoner Mobile Security v1.0.0 (Zoner).

From the testing results, we are shown that some software like Zoner detection rate to 99.4% (**Tables 5** and **6**, **Figure 8**).

5. Discussion

From the analysis of malware families and samples, the author saw that the ability to detect malware from the users is usually limited. The rapid development of new applications and variations to immune with mobile security software requires overall solution from the analysis of new variants and detect new viruses to alert the community, and then users should also take preventive measures:

Table 6. Result detect malware families (total).

Name / Detect	Dr. Web	Kaspersky	NetQin	Zoner
Num	1303	1045	479	1476
Time	742	2025	357	190

1) Users carefully read and understand permissions, an application and compare it with the real features of this app. In particular, users should not install or update software not necessary for the unknown effects of this app.

2) When an app is installed, users should check that the extraordinary can happen: no icon appears corresponding with this app (without, more one icon), Check

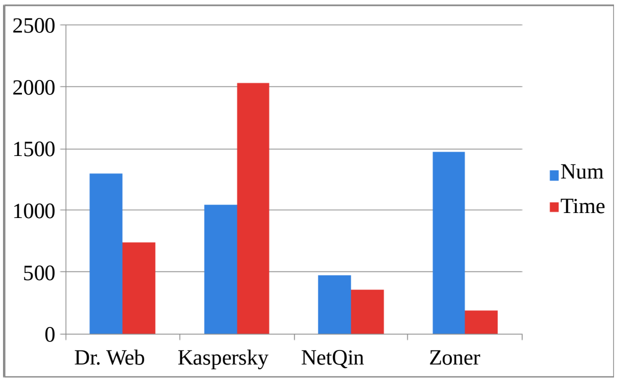


Figure 8. Result detect malware families (Chart).

regularly phone bill or account.

3) Users should invest a mobile security software copyright and install all apps from the official Android Market instead of third—party market.

4) Users should download an app with thousands of downloads and mostly positive comments.

5) Turn off unused features such as: GPS, GPRS, WIFI (Settings > Wireless & networks > Wi-Fi), extend memory (Settings -> Applications -> Development -> USB debugging), .… Especially, Android OS allows users to install file. APK in unknown sources directly and the malware easily penetrate the user's phone. (Settings -> Applications -> unknown sources).

6) Keep your phone patched up to date.

6. Conclusions

From the analysis of the characteristics of the collected malware samples, the author classified them into their existing families or their addition of a new family for their collection with 58 malware families and 1485 malware samples. And the author introduced three different techniques to analyze the sample introduced in Section 1.

The author selected the recognizable characteristics from ordinary users with their families that had collected (**Table 1**), and proposed solutions as recommendations to users before installing it with the ultimate desire to mitigate the damage in the community that is on the android phone, especially the ordinary users with limited understanding about potential hazards. The visible Symptoms of malware which exploit the device to gain root privilege are difficult to see and detect because they silently execute malicious code in the platform OS. Mostly, they steal information and send to remote server or URL by SMS messages (premium rate number or not).

The author presented evaluation results of the test 04 mobile security software of top ten software from AV-TEST in 2012 [51] with each family in order for the users to have the appropriate choice to proceed with fixing them and prevent them in the future, especially with malwares using root exploits when detecting the infection.

Beside, ordinary phone users recognize malwares by visible symptoms in order to fix it (**Table 4**) and they are careful when downloading and installing apps from official Android Market with security advisories (Section 5). If users are really concerned with the potential risks, they should consider investing in an effective mobile security app because it is still the best bet to stay protected anywhere, anytime. Also, when we are installing software of unknown source, the phones are also infected with malicious software before it can protect the phones.

REFERENCES

[1] UK, "Worldwide Mobile Device Sales to End Users by Operating System in third Quarter of 2012,"2012. http://www.gartner.com/it/page.jsp?id=2237315

[2] R. Thurner, "A Breakdown by Country of the Most Popular App Download Services to Help Make the Business Case," 2012. http://www.smartinsights.com/mobile-marketing/app-marketing/app-download-statistics/

[3] Kaspersky Lab, "The overall statistics for 2012," 2012. http://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012#1

[4] "Number of the Week: 40% of Modern Smartphones Owners Do Not Use Antivirus Software," 2012. http://www.kaspersky.com/about/news/ press/2012/number-of-the-week-40-percent-of-modern-smartphones-owners-do-not-use-antivirus-software

[5] Y. J. Zhou and X. X. Jiang, "Dissecting Android Malware: Characterization and Evolution," *Proceedings of the* 33*rd IEEE Symposium on Security and Privacy* (*Oakland* 2012), San Francisco, 20-23 May 2012, pp. 95-109.

[6] Contagio Mobile, "Download Malware Categories". http://contagiominidump.blogspot.com/

[7] US-CERT/NIST, "Vulnerability Summary for CVE-2009-1185," 2009. http://web.nvd.nist.gov/view/vuln/detail? vulnId= CVE-2009-1185

[8] X. X. Jiang, "Security Alert: New Sophisticated Android Malware DroidKungFu Found in Alternative Chinese App Markets," 2011. http://www.cs.ncsu.edu/faculty/jiang/DroidKungFu/

[9] X. X. Jiang, "Security Alert: New DroidKungFu Variants Found in Alternative Chinese Android Markets," 2011. http://www.cs.ncsu.edu/faculty/jiang/DroidKungFu2/

[10] X. X. Jiang, "Security Alert: New DroidKungFu Variant AGAIN! Found in Alternative Android Markets," 2011. http://www.csc.ncsu.edu/faculty/jiang/Droid KungFu3/

[11] Wikipedia, "Reverse_Engineering". http://en.wikipedia.org/wiki/ Reverse_engineering

[12] X. X. Jiang, "Security Alert: AnserverBot, New Sophisticated Android Bot Found in Alternative Android Markets," 2011.

http://www.csc.ncsu.edu/faculty/jiang/AnserverBot/

[13] Symantec, “Android.Basebridge,” 2011. http://www.symantec.com/ security_response/writeup.jsp?docid=2011-060915-4938-99 &tabid=2

[14] X. X. Jiang, “Security Alert: New BeanBot SMS Trojan Discovered,” 2011. http://www.csc.ncsu.edu/faculty/ jiang/BeanBot/

[15] Trendmicro, “ANDROIDOS_BGSERV.A,” 2011. http://about-threats. trendmicro.com/us/malware/AndroidOS_BGSERV.A

[16] Symantec, “Android.Pjapps,” 2011. http://www.symantec.com/securit yresponse/writeup.jsp?docid=2011-022303-3344-99&tabid=2

[17] M. Balanza, “Android Malware Acts as an SMS Relay,” Trend Labs, 2011. http://blog.trendmicro.com/trendlabs-security-intellige nce /android-malware-acts-as-an-sms-relay/

[18] NQMobile, “DroidCoupon”. http://labs.netqin.com/us/?p=112

[19] Kindsight Lab, Malware Analysis Report, “AndroidOS/ DroidDeluxe,” 2011. https://www.kindsight.net/ sites/default/files/Kindsight_Malware_Analysis-Android-Trojan-DroidDeluxe-final.pdf

[20] Lookout, “Technical Analysis DroidDream Malware,” 2011. https:// blog.lookout.com/droiddream/

[21] Trendmicro, “ANDROIDOS_DORDRAE.N,” 2011. http://about-threats.trendmicro.com/us/malware/ANDROIDOS_DORDRAE.N

[22] AVGbobilation, “Malware Information: DroidDreamLight,” 2011. http://cms.avg-hrd.appspot.com/securitycenter/securitypost_20110601.html

[23] X. X. Jiang, “Security Alert: New Sophisticated Android Malware Droid KungFu Found in Alternative Chinese App Markets,” 2011. http://www.cs.ncsu.edu/faculty/jiang/DroidKung Fu/

[24] X. X. Jiang, “Security Alert: Be Cautious with Android Spyware—GamblerSMS,” 2011. http://www.cs.ncsu.edu/ faculty/jiang/GamblerSMS/

[25] Symantec, “Android.Ggtracker,” 2011. http://www.symantec.com/ security_response/writeup.jsp?docid=2011-062208-5013-99&tabid= 2

[26] Symantec, “Android.Geinimi,” 2011. http://www.symantec.com/ security_response/writeup.jsp?docid=2011-010111-5403-99& tabid=-9

[27] AVGbobilation, “Malware information: GingerMaster”. http://cms.avg-hrd.appspot.com/securitycenter/securitypost_20110825.html#tabs-2

[28] Symantec, “Android.Golddream,” 2011. http://www.symantec.com/ security_response/writeup.jsp?docid=2011-070608-4139-99& tabid=2

[29] AVGbobilation, “Malware Information: Gone60,” 2011. http://cms.avg-hrd.appspot.com/securitycenter/securitypost_20110927.html#tabs-2

[30] Y. Takash, “Beta Version of Spytool App for Android Steals SMS Messages,” i, TrenLabs, 2012. http://blog.trend micro.com/trendlabs-security-intelligence/beta-version-of-spytool-app-for-android-steals-sms-messages/

[31] A. Apvrille, “QR Code and Mobile Malware: It Happened!” FortiBlog, 2011. http://blog.fortinet.com/qr-code-and-mobile- malware-it-happened/

[32] Mcafee, “Virus Profile: Android/J.SMSHider.A,” 2011. http://home. mcafee.com/VirusInfo/VirusProfile.aspx?key=527859#none

[33] Symantec, “LoveTrap” 2011. http://www.symantec.com/security_res ponse/writeup.jsp?docid=2011-072806-2905-99&tabid=2

[34] Symantec, “Android.Ozotshielder,” 2011. http://www.symantec.com /security_response/writeup.jsp?docid=2011-091505-3230-99

[35] AVGbobilation, “Malware Information: NickiSpy”. http://cms.avg-hrd.appspot.com/securitycenter/securitypost_20110804.htm#tabs-2

[36] M. Ballano, “Android Threats Getting Steamy,” 2011. http://www.symantec.com/connect/blogs/android-threats-getting-steamy

[37] X. Jiang, “Security Alert: New Stealthy Android Spyware—Plankton—Found in Official Android Market,” 2011. http://www.csc.ncsu.edu/faculty/jiang/Plankton/

[38] X. Jiang, “Security Alert: New Rogue App RogueLemon Found in Alternative Chinese Android Markets,” 2011. http://www.csc.ncsu.edu/faculty/jiang/RogueLemon/

[39] X. Jiang, “New Rogue Android App—Ro-gueSPPush—Found in Alternative Android Markets,” 2011 http://www.cs.ncsu.edu/faculty/jiang/RogueSPPush/

[40] Zimry, Irene, Raulf and Leong-F-Secure, “On Android threats Spyware: Android/SndApps.A and Trojan: Android/SmsSpy.D,” 2011. http://www.f-secure.com/weblog/archives/00002202.html

[41] Forensic Blog, “Detailed Analysis of Android.Spitmo,” 2011, http://forensics.spreitzenbarth.de/2011/12/06/detailed-analysis-of-android-spitmo/

[42] Symantec, “Walkinwat,” 2011. http://www.symantec.com/security_response/writeup.jsp?docid=2011-033008-4831-99&tabid=2

[43] Symantec, “Tapsnake,” 2010. http://www.symantec.com/security_response/writeup.jsp?docid=2010-081214-2657-99

[44] T. Strazzere, “Security Alert: Zsone Trojan Found in Android Market,” 2011. https://blog.lookout.com/blog/2011/05/11/security-alert-zsone-trojan-found-in-android-market

[45] Symantec, “Android.Counterclank,” 2012.

http://www.symantec.com/security_response/writeup.jsp?docid=2012-012709-4046-99&tabid=2

[46] Symantec, “Android.Dougalek,” 2012. http://www.symantec.com/security_response/writeup.jsp?docid=2012-041601-3400-99

[47] L. Arsene, “Android SMS Bot Uses Twitter to Hide C&C Server,” 2012. http://www.hotforsecurity.com/blog/android-sms-bot-uses-twitter-to-hide-cc-server-2602.html

[48] I. Asrar, “Android.Dropdialer Identified on Google Play,” 2012. http://www.symantec.com/connect/blogs/androiddrodialer-identified-google-play

[49] B. Botezatu, “From China with Love: New Android Backdoor Spreading through Hacked Apps,” 2012. http://www.hotforsecurity.com/blog/from-china-with-love-new-android-backdoor-spreading-through-hacked-apps-1317.html

[50] I. Asrar, “Scam Proves Privacy Concerns on Mobile Devices,” 2012. http://www.symantec.com/connect/blogs/scam-proves-privacy-concerns-mobile-devices-0

[51] AV-TEST, “Test Report: Anti-Malware solutions for Android,” 2012. http://www.av-test.org/en/tests/mobile-devices/android/

[52] Open Source Database of Android Malware (links + signatures), 2012 https://code.google.com/p/androguard/wiki/DatabaseAndroMawares#Open_Source_database_of_android_malwares